

India Telecom News

<http://indiatelecomnews.com/?p=1797>

Enterprises concerned with mobile security: Fortinet survey

Written by admin on 21 November 2011



A Fortinet-commissioned survey of 350 IT professionals in medium to large-sized enterprises across Asia has found that businesses are concerned about the comprehensive of security coverage and the cost of IT security implementation.

The survey queried enterprise IT decision makers in China, Hong Kong, India, Japan, Singapore, South Korea and Taiwan about their security strategies and priorities amid a rapidly changing IT landscape in which businesses try to keep pace with cloud computing and mobile device proliferation.

Re-Strategising for More Thorough Coverage, Lower Cost

When asked about their IT security strategy, respondents believe that the top two areas of improvement by far are comprehensiveness of coverage and cost of their IT security implementation. They want coverage to be extended beyond the core network perimeter to areas like mobile endpoints and processes, and they want security-related costs to be reduced. Of the seven markets surveyed, Singapore had the most respondents ranking comprehensiveness of coverage as their no.1 priority (71%), while Hong Kong had the most respondents citing cost effectiveness as their top concern (58%).

There are several drivers for the strategy changes. Heading the list are technologies under rapid adoption in Asia, including cloud computing (36% of respondents named it as the most important driver) and virtualisation (16%). Other influences shaping IT security strategy are the emergence of more sophisticated threats and attacks (15%), user-led IT (14%) and mobility (11%).

Enterprises Responding Faster to Changing Trends

In line with fast evolving trends, many organisations are assessing their IT security strategy frequently. As many as 74% of the respondents have conducted a full reappraisal of their information security strategy in the last 12 months.

“The remarkable pace of cloud computing adoption and the growing trend of employees plugging their personal devices to the corporate network are posing serious challenges to traditionally secured networks,” said Patrice Perche, Senior Vice President of International Sales and Support at Fortinet. “Organisations must evaluate their security posture in a timely manner, so that they can take immediate steps against new vulnerability points on the network, as well as secure new technologies that emerge. In that context, it is critical for them to revise their legacy security implementation and adopt solutions which can protect and control at the network, application and user levels.”

In fact, the survey unveiled that as many as 85% of respondents are concerned about their firms’ ability to secure corporate data in this new user-led IT environment, where individual users, rather than enterprises, define the preferred IT practices and technologies they wish to use. South Korean and Indian organisations are the most worried (both 94%) by this “IT consumerisation”. Japan is the least worried, but even there, almost two thirds of the respondents (63%) say they are concerned.

Inadequate Security for Personal Mobile Devices

Across the sample, 94% of respondents say that they have a mobile security strategy defined. Hong Kong and Taiwan are the most advanced markets in this area, both at 98%.

However, results indicate that most companies are not confident of or do not have the means to secure personal mobile devices: 67% of respondents say they only allow the use of corporate mobile devices onto which security policies can be directly enforced. Twenty-six percent of enterprises place responsibility for securing personal mobile endpoints directly with the users/owners of those devices ? a dangerous practice.

Wireless Networks: The Greatest Vulnerability

When asked about which parts of their IT infrastructure are vulnerable from a security standpoint, wireless networks are named most frequently (quoted by 59% of the respondents). In terms of severity of risk, wireless networks are also rated highest, ahead of endpoints (ranked 2nd) and databases (3rd). Wireless networks are seen as particularly vulnerable in Japan, with 86% of that country’s respondents ranking it as their top threat, ahead of South Korea (61%) and Hong Kong (55%).

Migration to Application Aware and XML Firewalls has Started

Today’s security threats are no longer port-based and can slip into enterprise networks through applications. With application awareness and control capabilities underpinning the emergence of ‘next-generation’ firewalls and the death of traditional firewalling solutions, 42% of the respondents are now using, or plan to use, a firewall with application control features.

Specialised Web application and XML firewalls are also being adopted in significant numbers, with 45% of the overall sample now using, or planning to use, this technology to secure Web-based applications.

- Singapore shows the highest rate of 'next generation' firewall adoption with 52% of its sample using this technology. India and South Korea follow closely, tying at 48%.
- China and Taiwan are the largest adopters of Web application /XML firewalls, with 61% and 48% of their samples, respectively. India is 3rd with 44%.

Network Security Consolidation Gathering Momentum

To date, almost three quarters (71%) of respondents have consolidated security elements to take advantage of tighter security, simplified management and lower cost, and 90% of them say that they will continue consolidating security over the next 12 months.

Twenty-six percent of the sampled organisations plan to embark on a network security consolidation exercise for the first time in the next 12 months. Only 3% of the respondents plan to continue abstaining from any network security consolidation in the foreseeable future.

- South Korea is the furthest ahead in the network security consolidation game, with 78% of respondents already having done some form of consolidation. China is 2nd with 77% and Taiwan is 3rd with 74%.
- In Japan, 14% of the sample feels they have embraced network security consolidation to the furthest extent desirable. This is twice as high as the Asian average of 7%.
- Hong Kong organisations are most likely to start out on network security consolidation for the first time (34%). Singapore is 2nd with 32%. In Japan, the figure is only 18%.

“IT departments and dedicated information security professionals face challenges from all directions as they fight to maintain a coherent security strategy that both protects data, and responds to the changing needs of users and the business at large,” added Perche. “Organisations that can call upon the common technology approach of an end-to-end security solution family are best set to meet these challenges without complicating management processes, compromising performance, or adding unnecessary financial overheads.”

(Courtesy: NetEvents)